THE BITCOIN STANDARD

THE BITCOIN STANDARD

The Decentralized Alternative to Central Banking

Saifedean Ammous

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data is Available:

ISBN 9781119473862 (Hardcover)
ISBN 9781119473893 (ePDF)
ISBN 9781119473916 (ePub)

Cover Design: Wiley
Cover Images: REI stone © Danita Delimont/Getty Images; gold bars © Grassetto/Getty Images; QR code/Courtesy of Saifedean Ammous

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

To my wife and daughter, who give me a reason to write.
And to Satoshi Nakamoto, who gave me something worth writing about.

Contents

About the Author

Saifedean Ammous is a Professor of Economics at the Lebanese American University and member of the Center on Capitalism and Society at Columbia University. He holds a PhD in Sustainable Development from Columbia University.

Foreword

by Nassim Nicholas Taleb

Let us follow the logic of things from the beginning. Or, rather, from the end: modern times. We are, as I am writing these lines, witnessing a complete riot against some class of experts, in domains that are too difficult for us to understand, such as macroeconomic reality, and in which not only is the expert not an expert, but he doesn't know it. That previous Federal Reserve bosses Greenspan and Bernanke, had little grasp of empirical reality is something we only discovered too late: one can macroBS longer than microBS, which is why we need to be careful of whom to endow with centralized macro decisions.

What makes it worse is that all central banks operated under the same model, making it a perfect monoculture.

In complex domains, expertise doesn't concentrate: under organic reality, things work in a distributed way, as F. A. Hayek has convincingly demonstrated. But Hayek used the notion of distributed knowledge. Well, it looks like we do not even need the "knowledge" part for things to work well. Nor do we need individual rationality. All we need is structure.

It doesn't mean all participants have a democratic share in decisions. One motivated participant can disproportionately move the needle (what I have studied as the asymmetry of the minority rule). But every participant has the option to be that player.

Somehow, under scale transformation, a miraculous effect emerges: rational markets do not require any individual trader to be rational. In fact they work well under zero intelligence—a zero-intelligence crowd, under the right design, works better than a Soviet-style management composed of maximally intelligent humans.

Which is why Bitcoin is an excellent idea. It fulfills the needs of the complex system, not because it is a cryptocurrency, but precisely because it has no owner, no authority that can decide on its fate. It is owned by the crowd, its users. And it now has a track record of several years, enough for it to be an animal in its own right.

For other cryptocurrencies to compete, they need to have such a Hayekian property.

Bitcoin is a currency without a government. But, one may ask, didn't we have gold, silver, and other metals, another class of currencies without a government? Not quite. When you trade gold, you trade "loco" Hong Kong and end up receiving a claim on a stock there, which you might need to move to New Jersey. Banks control the custodian game and governments control banks (or, rather, bankers and government officials are, to be polite, tight together). So Bitcoin has a huge advantage over gold in transactions: clearance does not require a specific custodian. No government can control what code you have in your head.

Finally, Bitcoin will go through hiccups. It may fail; but then it will be easily reinvented as we now know how it works. In its present state, it may not be convenient for transactions, not good enough to buy your decaffeinated espresso macchiato at your local virtue-signaling coffee chain. It may be too volatile to be a currency for now. But it is the first organic currency.

But its mere existence is an insurance policy that will remind governments that the last object the establishment could control, namely, the currency, is no longer their monopoly. This gives us, the crowd, an insurance policy against an Orwellian future.

Nassim Nicholas Taleb
January 22, 2018

Prologue

On November 1, 2008, a computer programmer going by the pseudonym Satoshi Nakamoto sent an email to a cryptography mailing list to announce that he had produced a "new electronic cash system that's fully peer-to-peer, with no trusted third party."[1] He copied the abstract of the paper explaining the design, and a link to it online. In essence, Bitcoin offered a payment network with its own native currency, and used a sophisticated method for members to verify all transactions without having to trust in any single member of the network. The currency was issued at a predetermined rate to reward the members who spent their processing power on verifying the transactions, thus providing a reward for their work. The startling thing about this invention was that, contrary to many other previous attempts at setting up a digital cash, it actually worked.

While a clever and neat design, there wasn't much to suggest that such a quirky experiment would interest anyone outside the circles of cryptography geeks. For months this was the case, as barely a few dozen users worldwide were joining the network and engaging in mining and

[1] The full email can be found on the Satoshi Nakamoto Institute archive of all known Satoshi Nakamoto writings, available at www.nakamotoinstitute.org

sending each other coins that began to acquire the status of collectibles, albeit in digital form.

But in October 2009, an Internet exchange[2] sold 5,050 bitcoins for $5.02, at a price of $1 for 1,006 bitcoins, to register the first purchase of a bitcoin with money.[3] The price was calculated by measuring the value of the electricity needed to produce a bitcoin. In economic terms, this seminal moment was arguably the most significant in Bitcoin's life. Bitcoin was no longer just a digital game being played within a fringe community of programmers; it had now become a market good with a price, indicating that someone somewhere had developed a positive valuation for it. On May 22, 2010, someone else paid 10,000 bitcoins to buy two pizza pies worth $25, representing the first time that bitcoin was used as a medium of exchange. The token had needed seven months to transition from being a market good to being a medium of exchange.

Since then, the Bitcoin network has grown in the number of users and transactions, and the processing power dedicated to it, while the value of its currency has risen quickly, exceeding $7,000 per bitcoin as of November 2017.[4] After eight years, it is clear that this invention is no longer just an online game, but a technology that has passed the market test and is being used by many for real-world purposes, with its exchange rate being regularly featured on TV, in newspapers, and on websites along with the exchange rates of national currencies.

Bitcoin can be best understood as distributed software that allows for transfer of value using a currency protected from unexpected inflation without relying on trusted third parties. In other words, Bitcoin automates the functions of a modern central bank and makes them predictable and virtually immutable by programming them into code decentralized among thousands of network members, none of whom can alter the code without the consent of the rest. This makes Bitcoin the first demonstrably reliable operational example of *digital cash* and *digital hard money*. While Bitcoin is a new invention of the digital age, the problems it purports to solve—namely, providing a form of money that is

[2]The now-defunct New Liberty Standard.

[3]Nathaniel Popper, *Digital Gold* (Harper, 2015).

[4]In other words, in the eight years it has been a market commodity, a bitcoin has appreciated around almost eight million-fold, or, precisely 793,513,944% from its first price of $0.000994 to its all-time high at the time of writing, $7,888.

under the full command of its owner and likely to hold its value in the long run—are as old as human society itself. This book presents a conception of these problems based on years of studying this technology and the economic problems it solves, and how societies have previously found solutions for them throughout history. My conclusion may surprise those who label Bitcoin a scam or ruse of speculators and promoters out to make a quick buck. Indeed, Bitcoin improves on earlier "store of value" solutions, and Bitcoin's suitability as the sound money of a digital age may catch naysayers by surprise.

History can foreshadow what's to come, particularly when examined closely. And time will tell just how sound the case made in this book is. As it must, the first part of the book explains money, its function and properties. As an economist with an engineering background, I have always sought to understand a technology in terms of the problems it purports to solve, which allows for the identification of its functional essence and its separation from incidental, cosmetic, and insignificant characteristics. By understanding the problems money attempts to solve, it becomes possible to elucidate what makes for sound and unsound money, and to apply that conceptual framework to understand how and why various goods, such as seashells, beads, metals, and government money, have served the function of money, and how and why they may have failed at it or served society's purposes to store value and exchange it.

The second part of the book discusses the individual, social, and global implications of sound and unsound forms of money throughout history. Sound money allows people to think about the long term and to save and invest more for the future. Saving and investing for the long run are the key to capital accumulation and the advance of human civilization. Money is the information and measurement system of an economy, and sound money is what allows trade, investment, and entrepreneurship to proceed on a solid basis, whereas unsound money throws these processes into disarray. Sound money is also an essential element of a free society as it provides for an effective bulwark against despotic government.

The third section of the book explains the operation of the Bitcoin network and its most salient economic characteristics, and analyzes the possible uses of Bitcoin as a form of sound money, discussing some use

cases which Bitcoin does not serve well, as well as addressing some of the most common misunderstandings and misconceptions surrounding it.

This book is written to help the reader understand the economics of Bitcoin and how it serves as the digital iteration of the many technologies used to fulfill the functions of money throughout history. This book is not an advertisement or invitation to buy into the bitcoin currency. Far from it. The value of bitcoin is likely to remain volatile, at least for a while; the Bitcoin network may yet succeed or fail, for whatever foreseeable or unforeseeable reasons; and using it requires technical competence and carries risks that make it unsuited for many people. This book does not offer investment advice, but aims at helping elucidate the economic properties of the network and its operation, to allow readers an informed understanding before deciding whether they want to use it.

Only with such an understanding, and only after extensive and thorough research into the practical operational aspects of owning and storing bitcoins, should anyone consider holding value in Bitcoin. While bitcoin's rise in market value may make it appear like a no-brainer as an investment, a closer look at the myriad hacks, attacks, scams, and security failures that have cost people their bitcoins provides a sobering warning to anyone who thinks that owning bitcoins provides a guaranteed profit. Should you come out of reading this book thinking that the bitcoin currency is something worth owning, your first investment should not be in buying bitcoins, but in time spent understanding how to buy, store, and own bitcoins securely. It is the inherent nature of Bitcoin that such knowledge cannot be delegated or outsourced. There is no alternative to personal responsibility for anyone interested in using this network, and that is the real investment that needs to be made to get into Bitcoin.

Chapter 1

Money

Bitcoin is the newest technology to serve the function of money—an invention leveraging the technological possibilities of the digital age to solve a problem that has persisted for all of humanity's existence: how to move economic value across time and space. In order to understand Bitcoin, one must first understand money, and to understand money, there is no alternative to the study of the function and history of money.

The simplest way for people to exchange value is to exchange valuable goods with one another. This process of *direct exchange* is referred to as barter, but is only practical in small circles with only a few goods and services produced. In a hypothetical economy of a dozen people isolated from the world, there is not much scope for specialization and trade, and it would be possible for individuals to each engage in the production of the most basic essentials of survival and exchange them among themselves directly. Barter has always existed in human society and continues to this day, but it is highly impractical and remains only in